



Eseguire il backup dei database Oracle nativi del cloud

BlueXP backup and recovery

NetApp
April 18, 2024

Sommario

- Eseguire il backup dei database Oracle nativi del cloud 1
 - Avvio rapido 1
 - Configurare FSX per ONTAP 2
 - Configurare Cloud Volumes ONTAP 3
 - Configurare Azure NetApp Files. 3
 - Installare il plug-in SnapCenter per Oracle e aggiungere host di database. 4
 - Eseguire il backup dei database Oracle nativi del cloud 11

Eseguire il backup dei database Oracle nativi del cloud

Avvio rapido

Inizia subito seguendo questa procedura.

1

Verificare il supporto per la configurazione

- Sistema operativo:
 - RHEL 7.5 o versione successiva e 8.x.
 - OL 7.5 o versione successiva e 8.x
 - SLES 15 SP4
- Cloud storage NetApp:
 - Amazon FSX per NetApp ONTAP
 - Cloud Volumes ONTAP
 - Azure NetApp Files
- Layout dello storage:
 - NFS v3 e v4.1 (incluso DNFS)
 - iSCSI con ASM (ASMFD, ASMLib e ASMUdev)



Azure NetApp Files non supporta l'ambiente SAN.

- Layout dei database: Oracle Standard e Oracle Enterprise standalone (CDB e PDB legacy e multi-tenant)
- Versioni di database: 19c e 21c

2

Iscriviti a BlueXP

BlueXP è accessibile da una console basata su web. Una volta iniziato a utilizzare BlueXP, il primo passo consiste nell'isciversi utilizzando le credenziali del sito di supporto NetApp o creando un login cloud NetApp. Per ulteriori informazioni, fare riferimento a. "[Iscriviti a BlueXP](#)".

3

Accedere a BlueXP

Dopo aver effettuato la registrazione a BlueXP, è possibile accedere dalla console basata sul Web. Per ulteriori informazioni, fare riferimento a. "[Accedere a BlueXP](#)".

4

Gestisci il tuo account BlueXP

Puoi amministrare il tuo account gestendo utenti, account di servizio, aree di lavoro e connettori. Per ulteriori informazioni, fare riferimento a. "[Gestisci il tuo account BlueXP](#)".

Configurare FSX per ONTAP

Con BlueXP è necessario creare un ambiente di lavoro FSX per ONTAP per aggiungere e gestire volumi e servizi dati aggiuntivi. È inoltre necessario creare un connettore in AWS che consenta a BlueXP di gestire risorse e processi all'interno del proprio ambiente di cloud pubblico.

Creare un ambiente di lavoro FSX per ONTAP

È necessario creare FSX per ambienti di lavoro ONTAP in cui sono ospitati i database. Per ulteriori informazioni, fare riferimento a ["Inizia a utilizzare Amazon FSX per ONTAP"](#) e ["Creare e gestire un ambiente di lavoro Amazon FSX per ONTAP"](#).

È possibile creare l'ambiente di lavoro FSX per ONTAP utilizzando BlueXP o AWS. Se hai creato utilizzando AWS, dovresti scoprire FSX per i sistemi ONTAP in BlueXP.

Creare un connettore

Un account Admin deve creare un connettore in AWS che consenta a BlueXP di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Per ulteriori informazioni, fare riferimento a ["Creazione di un connettore in AWS da BlueXP"](#).

- È necessario utilizzare lo stesso connettore per gestire sia l'ambiente di lavoro FSX per ONTAP che i database.
- Se si dispone dell'ambiente di lavoro FSX per ONTAP e dei database nello stesso cloud privato virtuale (VPC), è possibile implementare il connettore nello stesso VPC.
- Se si dispone dell'ambiente di lavoro FSX per ONTAP e di database in diversi VPC:
 - Se si dispone di carichi di lavoro NAS (NFS) configurati su FSX per ONTAP, è possibile creare il connettore su uno dei VPC.
 - Se si hanno solo carichi di lavoro SAN configurati e non si intende utilizzare carichi di lavoro NAS (NFS), è necessario creare il connettore nel VPC in cui viene creato il sistema FSX per ONTAP.



Per utilizzare i carichi di lavoro NAS (NFS), è necessario disporre di un gateway di transito tra il VPC del database e Amazon VPC. È possibile accedere all'indirizzo IP NFS, che è un indirizzo IP mobile, da un altro VPC solo attraverso il gateway di transito. Non è possibile accedere agli indirizzi IP mobili eseguendo il peering dei VPC.

Dopo aver creato il connettore, fare clic su **Storage > Canvas > My Working Environments > Add Working Environment** (Aggiungi ambiente di lavoro) e seguire le istruzioni per aggiungere l'ambiente di lavoro. Assicurarsi che vi sia connettività dal connettore agli host del database Oracle e all'ambiente di lavoro FSX. Il connettore dovrebbe essere in grado di connettersi all'indirizzo IP di gestione del cluster dell'ambiente di lavoro FSX.

- Aggiungere l'ambiente di lavoro facendo clic su **Storage > Canvas > My Working Environments > Add Working Environment**.

Assicurarsi che vi sia connettività dal connettore agli host del database e all'ambiente di lavoro FSX per ONTAP. Il connettore deve connettersi all'indirizzo IP di gestione del cluster di FSX per l'ambiente di lavoro ONTAP.

- Copiare l'ID del connettore facendo clic su **Connector > Manage Connectors** (connettore > Gestisci connettori) e selezionando il nome del connettore.

Configurare Cloud Volumes ONTAP

Con BlueXP è necessario creare un ambiente di lavoro Cloud Volumes ONTAP per aggiungere e gestire volumi e servizi dati aggiuntivi. È inoltre necessario creare un connettore per il proprio ambiente cloud che consenta a BlueXP di gestire risorse e processi all'interno del proprio ambiente di cloud pubblico.

Creare un ambiente di lavoro Cloud Volumes ONTAP

È possibile individuare e aggiungere sistemi Cloud Volumes ONTAP esistenti a BlueXP. Per ulteriori informazioni, fare riferimento a ["Aggiunta di sistemi Cloud Volumes ONTAP esistenti a BlueXP"](#).

Creare un connettore

Puoi iniziare a utilizzare Cloud Volumes ONTAP per il tuo ambiente cloud in pochi passaggi. Per ulteriori informazioni, fare riferimento a una delle seguenti voci:

- ["Avvio rapido di Cloud Volumes ONTAP in AWS"](#)
- ["Avvio rapido di Cloud Volumes ONTAP in Azure"](#)
- ["Guida rapida per Cloud Volumes ONTAP in Google Cloud"](#)

È necessario utilizzare lo stesso connettore per gestire sia l'ambiente di lavoro Cloud Volumes ONTAP che i database.

- Se l'ambiente di lavoro Cloud Volumes ONTAP e i database si trovano nello stesso cloud privato virtuale (VPC) o VNET, è possibile implementare il connettore nello stesso VPC o VNET.
- Se si dispone di un ambiente di lavoro Cloud Volumes ONTAP e di database in VPC o VNet diversi, assicurarsi che i VPC o VNet siano peering.

Configurare Azure NetApp Files

Con BlueXP è necessario creare un ambiente di lavoro Azure NetApp Files per aggiungere e gestire volumi e servizi dati aggiuntivi. È inoltre necessario creare un connettore in Azure che consenta a BlueXP di gestire risorse e processi all'interno del proprio ambiente di cloud pubblico.

Creare un ambiente di lavoro Azure NetApp Files

È necessario creare ambienti di lavoro Azure NetApp Files in cui sono ospitati i database. Per ulteriori informazioni, fare riferimento a ["Scopri di più su Azure NetApp Files"](#) e ["Creare un ambiente di lavoro Azure NetApp Files"](#).

Creare un connettore

Un amministratore di account BlueXP dovrebbe implementare un connettore in Azure che consenta a BlueXP di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Per ulteriori informazioni, fare riferimento a. ["Creare un connettore in Azure da BlueXP"](#).

- Assicurarsi che vi sia connettività tra il connettore e gli host del database.
- Se si dispone dell'ambiente di lavoro e dei database Azure NetApp Files nella stessa rete virtuale (VNET), è possibile implementare il connettore nella stessa rete virtuale.
- Se si dispone di un ambiente di lavoro Azure NetApp Files e di database in reti VNet diverse e si hanno carichi di lavoro NAS (NFS) configurati su Azure NetApp Files, è possibile creare il connettore su una delle reti VNet.

Dopo aver creato il connettore, aggiungere l'ambiente di lavoro facendo clic su **Storage > Canvas > My Working Environments > Add Working Environment**.

Installare il plug-in SnapCenter per Oracle e aggiungere host di database

È necessario installare il plug-in SnapCenter per Oracle su ciascuno degli host di database Oracle, aggiungere gli host di database e rilevare i database sull'host per assegnare criteri e creare backup.

- Se SSH è attivato per l'host del database, è possibile installare il plug-in utilizzando uno dei seguenti metodi:
 - Installare il plug-in e aggiungere l'host dall'interfaccia utente utilizzando l'opzione SSH. [Scopri di più](#).
 - Installare il plug-in utilizzando lo script e aggiungere l'host dall'interfaccia utente utilizzando l'opzione manuale. [Scopri di più](#).
- Se SSH è disattivato, installare il plug-in manualmente e aggiungere l'host dall'interfaccia utente utilizzando l'opzione manuale. [Scopri di più](#).

Prerequisiti

Prima di aggiungere l'host, assicurarsi che i prerequisiti siano soddisfatti.

- L'ambiente di lavoro e il connettore dovrebbero essere stati creati.
- Assicurarsi che il connettore sia collegato agli host del database Oracle.

Per informazioni su come risolvere il problema di connettività, fare riferimento a. ["Impossibile convalidare la connettività dall'host del connettore BlueXP all'host del database dell'applicazione"](#).

Quando il connettore viene perso o se è stato creato un nuovo connettore, è necessario associarlo alle risorse dell'applicazione esistenti. Per istruzioni sull'aggiornamento del connettore, vedere ["Aggiornare i dettagli del connettore"](#).

- Assicurarsi che l'utente BlueXP abbia il ruolo di "account Admin".
- Assicurarsi che l'account non root (sudo) sia presente sull'host dell'applicazione per le operazioni di protezione dei dati.
- Assicurarsi che Java 11 (64-bit) Oracle Java o OpenJDK sia installato su ciascuno degli host di database Oracle e che LA variabile JAVA_HOME sia impostata correttamente.
- Se viene eseguita l'installazione basata su SSH, assicurarsi che il connettore abbia attivato la comunicazione con la porta SSH (impostazione predefinita: 22).

- Assicurarsi che il connettore abbia la comunicazione abilitata alla porta plug-in (impostazione predefinita: 8145) per il funzionamento delle operazioni di protezione dei dati.
- Assicurarsi che sia installata la versione più recente del plug-in. Per aggiornare il plug-in, fare riferimento a [Upgrade del plug-in SnapCenter per database Oracle](#).

Aggiungere host dall'interfaccia utente utilizzando l'opzione SSH

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection > Backup and Recovery > Applications**.

Se è già stato aggiunto un host e si desidera aggiungere un altro host, fare clic su **applicazioni > Gestisci database > Aggiungi**, quindi passare al punto 5.

2. Fare clic su **Scopri applicazioni**.
3. Selezionare **Cloud Native** e fare clic su **Next**.

Viene creato un account di servizio (*SnapCenter-account-`<accountid>`*) con ruolo *sistema SnapCenter* per eseguire operazioni pianificate di protezione dei dati per tutti gli utenti di questo account. L'account del servizio (*SnapCenter-account-`<accountid>`*) viene utilizzato per eseguire le operazioni di backup pianificate. Non eliminare mai l'account del servizio. Per visualizzare l'account del servizio, fare clic su **account > Gestisci account > membri**.

4. Selezionare Oracle come tipo di applicazione.
5. Nella pagina host details (Dettagli host), eseguire le seguenti operazioni:

- a. Selezionare **utilizzando SSH**.
- b. Specificare l'FQDN o l'indirizzo IP dell'host in cui si desidera installare il plug-in.

Assicurarsi che il connettore sia in grado di comunicare con l'host del database utilizzando l'FQDN o l'indirizzo IP.

- c. Specificare l'utente non root(sudo) che utilizza il pacchetto del plug-in da copiare sull'host.

L'utente root non è supportato.

- d. Specificare la porta SSH e il plug-in.

La porta SSH predefinita è 22 e la porta plug-in è 8145.

Dopo aver installato il plug-in, è possibile chiudere la porta SSH sull'host dell'applicazione. La porta SSH non è necessaria per le operazioni di protezione dei dati.

- a. Selezionare il connettore.
- b. (Facoltativo) se l'autenticazione senza chiave non è abilitata tra il connettore e l'host, specificare la chiave privata SSH che verrà utilizzata per comunicare con l'host.



La chiave privata SSH non viene memorizzata nell'applicazione e non viene utilizzata per altre operazioni.

- c. Fare clic su **Avanti**.

6. Nella pagina di configurazione, eseguire le seguenti operazioni:

- a. Configurare l'accesso sudo per l'utente SnapCenter nell'host del database Oracle effettuando l'accesso alla macchina Linux che esegue il database Oracle.
 - b. Copiare il testo visualizzato nell'interfaccia utente di BlueXP.
 - c. Creare il file `/etc/sudoers.d/snapcenter` sulla macchina Linux e incollare il testo copiato.
 - d. Nell'interfaccia utente di BlueXP, selezionare la casella di controllo e fare clic su **Avanti**.
7. Esaminare i dettagli e fare clic su **Scopri applicazioni**.
- Una volta installato il plug-in, viene avviata l'operazione di rilevamento.
 - Al termine dell'operazione di rilevamento, vengono visualizzati tutti i database sull'host. Se l'autenticazione del sistema operativo per il database è disattivata, fare clic su **Configura** per attivare l'autenticazione del database. Per ulteriori informazioni, fare riferimento a [Configurare le credenziali del database Oracle](#).
 - Fare clic su **Impostazioni** e selezionare **host** per visualizzare tutti gli host.
 - Fare clic su **Impostazioni** e selezionare **Criteri** per visualizzare i criteri predefiniti. Esaminare le policy predefinite e modificarle per soddisfare i requisiti o creare una nuova policy.

Aggiungere host dall'interfaccia utente utilizzando l'opzione manuale e installare il plug-in utilizzando lo script

Configurare l'autenticazione basata su chiave SSH per l'account utente non root dell'host Oracle ed eseguire i seguenti passaggi per installare il plug-in.

Prima di iniziare

Assicurarsi che la connessione SSH al connettore sia attivata.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection > Backup and Recovery > Applications**.
2. Fare clic su **Scopri applicazioni**.
3. Selezionare **Cloud Native** e fare clic su **Next**.

Viene creato un account di servizio (*SnapCenter-account-`<accountid>`*) con ruolo *sistema SnapCenter* per eseguire operazioni pianificate di protezione dei dati per tutti gli utenti di questo account. L'account del servizio (*SnapCenter-account-`<accountid>`*) viene utilizzato per eseguire le operazioni di backup pianificate. Non eliminare mai l'account del servizio. Per visualizzare l'account del servizio, fare clic su **account > Gestisci account > membri**.

4. Selezionare Oracle come tipo di applicazione.
5. Nella pagina host details (Dettagli host), eseguire le seguenti operazioni:
 - a. Selezionare **Manuale**.
 - b. Specificare l'FQDN o l'indirizzo IP dell'host in cui è installato il plug-in.

Assicurarsi che il connettore sia in grado di comunicare con l'host del database utilizzando l'FQDN o l'indirizzo IP.

- c. Specificare la porta del plug-in.

La porta predefinita è 8145.

- d. Specificare l'utente non root (sudo) che utilizza il pacchetto del plug-in da copiare sull'host.

- e. Selezionare il connettore.
 - f. Selezionare la casella di controllo per confermare che il plug-in è installato sull'host.
 - g. Fare clic su **Avanti**.
6. Nella pagina di configurazione, eseguire le seguenti operazioni:
- a. Configurare l'accesso sudo per l'utente SnapCenter nell'host del database Oracle effettuando l'accesso alla macchina Linux che esegue il database Oracle.
 - b. Copiare il testo visualizzato nell'interfaccia utente di BlueXP.
 - c. Creare il file `/etc/sudoers.d/snapcenter` sulla macchina Linux e incollare il testo copiato.
 - d. Nell'interfaccia utente di BlueXP, selezionare la casella di controllo e fare clic su **Avanti**.
7. Accedere a Connector VM.
8. Installare il plug-in utilizzando lo script fornito nel connettore.

```
sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
--host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
--pluginport <plugin_port> --sshport <host_ssh_port>
```

Se si utilizza un connettore meno recente, eseguire il seguente comando per installare il plug-in.

```
sudo
/var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name>
--sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
```

Nome	Descrizione	Obbligatorio	Predefinito
plugin_host	Specifica l'host Oracle	Sì	-
nome_utente_host	Specifica l'utente SnapCenter con privilegi SSH sull'host Oracle	Sì	-
host_ssh_key	Specifica la chiave SSH dell'utente SnapCenter e viene utilizzata per connettersi all'host Oracle	Sì	-
porta_plugin	Specifica la porta utilizzata dal plug-in	No	8145
host_ssh_port	Specifica la porta SSH sull'host Oracle	No	22

Ad esempio:

```
° sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
--host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk
```

- `sudo`
`/var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_pl`
`ugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey`
`/keys/netapp-ssh.ppk`

9. Nell'interfaccia utente di BlueXP, esaminare i dettagli e fare clic su **Scopri applicazioni**.

- Al termine dell'operazione di rilevamento, vengono visualizzati tutti i database sull'host. Se l'autenticazione del sistema operativo per il database è disattivata, fare clic su **Configura** per attivare l'autenticazione del database. Per ulteriori informazioni, fare riferimento a [Configurare le credenziali del database Oracle](#).
- Fare clic su **Impostazioni** e selezionare **host** per visualizzare tutti gli host.
- Fare clic su **Impostazioni** e selezionare **Criteri** per visualizzare i criteri predefiniti. Esaminare le policy predefinite e modificarle per soddisfare i requisiti o creare una nuova policy.

Aggiungere host dall'interfaccia utente utilizzando l'opzione manuale e installare il plug-in manualmente

Se l'autenticazione basata su chiave SSH non è abilitata sull'host del database Oracle, attenersi alla seguente procedura manuale per installare il plug-in e aggiungere l'host dall'interfaccia utente utilizzando l'opzione manuale.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection > Backup and Recovery > Applications**.
2. Fare clic su **Scopri applicazioni**.
3. Selezionare **Cloud Native** e fare clic su **Next**.

Viene creato un account di servizio (*SnapCenter-account-`<accountid>`*) con ruolo *sistema SnapCenter* per eseguire operazioni pianificate di protezione dei dati per tutti gli utenti di questo account. L'account del servizio (*SnapCenter-account-`<accountid>`*) viene utilizzato per eseguire le operazioni di backup pianificate. Non eliminare mai l'account del servizio. Per visualizzare l'account del servizio, fare clic su **account > Gestisci account > membri**.

4. Selezionare Oracle come tipo di applicazione.
5. Nella pagina **Dettagli host**, eseguire le seguenti operazioni:
 - a. Selezionare **Manuale**.
 - b. Specificare l'FQDN o l'indirizzo IP dell'host in cui è installato il plug-in.

Assicurarsi che il connettore sia in grado di comunicare con l'host del database utilizzando l'FQDN o l'indirizzo IP.

- c. Specificare la porta del plug-in.

La porta predefinita è 8145.

- d. Specificare l'utente sudo non-root (sudo) che utilizza il pacchetto del plug-in da copiare sull'host.
- e. Selezionare il connettore.
- f. Selezionare la casella di controllo per confermare che il plug-in è installato sull'host.
- g. Fare clic su **Avanti**.

6. Nella pagina di configurazione, eseguire le seguenti operazioni:

- a. Configurare l'accesso sudo per l'utente SnapCenter nell'host del database Oracle effettuando l'accesso alla macchina Linux che esegue il database Oracle.
 - b. Copiare il testo visualizzato nell'interfaccia utente di BlueXP.
 - c. Creare il file `/etc/sudoers.d/snapcenter` sulla macchina Linux e incollare il testo copiato.
 - d. Nell'interfaccia utente di BlueXP, selezionare la casella di controllo e fare clic su **Avanti**.
7. Accedere a Connector VM.
 8. Scarica il binario del plug-in host Linux di SnapCenter.

```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET 'http://127.0.0.1/deploy/downloadLinuxPlugin'
```

Il binario del plug-in è disponibile all'indirizzo: `cd /var/lib/docker/Volumes/service-manager[1]-2_cloudmanager_scs_cloud_volume/_data/$(sudo docker ps|grep -po "cloudmanager_scs_cloud:.?*"|sed -e/ */|cut -f2 -d":")/sc-linux-host-plugin`
 9. Copiare `snapcenter_linux_host_plugin_scs.bin` dal percorso sopra indicato al percorso `/home/<non root user (sudo)>/.sc_netapp` per ciascuno degli host di database Oracle utilizzando metodi scp o altri metodi alternativi.
 10. Accedere all'host del database Oracle utilizzando l'account non root (sudo).
 11. Modificare la directory in `/home/<non root user>/.sc_netapp/` ed eseguire il seguente comando per abilitare le autorizzazioni di esecuzione per il file binario.

```
chmod +x snapcenter_linux_host_plugin_scs.bin
```
 12. Installare il plug-in Oracle come utente sudo SnapCenter.

```
./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
```
 13. Copiare `certificate.pem` dal percorso `<base_mount_path>/client/certificate/` del connettore VM a `/var/opt/snapcenter/spl/etc/` sull'host plug-in.
 14. Andare a `/var/opt/snapcenter/spl/etc` ed eseguire il comando `keytool` per importare il file `certificate.pem`.

```
keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks -deststorepass snapcenter -noprompt
```
 15. Riavviare SPL: `systemctl restart spl`
 16. Verificare che il plug-in sia raggiungibile dal connettore eseguendo il comando riportato di seguito dal connettore.

```
docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the plug-in host>:<plug-in port>/PluginService/Version --cert /config/client/certificate/certificate.pem --key /config/client/certificate/key.pem
```
 17. Nell'interfaccia utente di BlueXP, esaminare i dettagli e fare clic su **Scopri applicazioni**.
 - Al termine dell'operazione di rilevamento, vengono visualizzati tutti i database sull'host. Se l'autenticazione del sistema operativo per il database è disattivata, fare clic su **Configura** per attivare l'autenticazione del database. Per ulteriori informazioni, fare riferimento a [Configurare le credenziali del database Oracle](#).
 - Fare clic su **Impostazioni** e selezionare **host** per visualizzare tutti gli host.
 - Fare clic su **Impostazioni** e selezionare **Criteri** per visualizzare i criteri predefiniti. Esaminare le policy predefinite e modificarle per soddisfare i requisiti o creare una nuova policy.

Configurare le credenziali del database Oracle

È necessario configurare le credenziali del database utilizzate per eseguire operazioni di protezione dei dati sui database Oracle.

Fasi

1. Se l'autenticazione del sistema operativo per il database è disattivata, fare clic su **Configura** per modificare l'autenticazione del database.
2. Specificare il nome utente, la password e i dettagli della porta.

Se il database risiede in ASM, è necessario configurare anche le impostazioni ASM.

L'utente Oracle deve disporre dei privilegi sysdba e l'utente ASM deve disporre dei privilegi sysasm.

3. Fare clic su **Configura**.

Upgrade del plug-in SnapCenter per database Oracle

È necessario aggiornare il plug-in SnapCenter per Oracle per accedere alle nuove funzionalità e ai miglioramenti più recenti. È possibile eseguire l'aggiornamento dall'interfaccia utente di BlueXP o dalla riga di comando.

Prima di iniziare

- Assicurarsi che non vi siano operazioni in esecuzione sull'host.

Fasi

1. Fare clic su **Backup and Recovery > applicazioni > host**.
2. Verificare se l'aggiornamento del plug-in è disponibile per uno degli host controllando la colonna Stato generale.
3. Aggiornare il plug-in dall'interfaccia utente o utilizzando la riga di comando.

Eseguire l'aggiornamento utilizzando l'interfaccia utente	Eseguire l'aggiornamento utilizzando la riga di comando
<p>a. Fare clic su ... Corrispondente all'host e fare clic su Upgrade Plug-in.</p> <p>b. Nella pagina di configurazione, eseguire le seguenti operazioni:</p> <ol style="list-style-type: none"> Configurare l'accesso sudo per l'utente SnapCenter nell'host del database Oracle effettuando l'accesso alla macchina Linux che esegue il database Oracle. Copiare il testo visualizzato nell'interfaccia utente di BlueXP. Modificare il file <code>/etc/sudoers.d/snapcenter</code> sulla macchina Linux e incollare il testo copiato. Nell'interfaccia utente di BlueXP, selezionare la casella di controllo e fare clic su Upgrade (Aggiorna). 	<p>a. Accedere a Connector VM.</p> <p>b. Eseguire il seguente script.</p> <pre>sudo /var/lib/docker/volumes/service- manager- 2_cloudmanager_scs_cloud_volume/_da ta/scripts/linux_plugin_copy_and_in stall.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade</pre> <p>Se si utilizza un connettore meno recente, eseguire il seguente comando per aggiornare il plug-in.</p> <pre>sudo /var/lib/docker/volumes/cloudmanage r_scs_cloud_volume/_data/scripts/li nux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade</pre>

Eseguire il backup dei database Oracle nativi del cloud

È possibile creare backup pianificati o on-demand assegnando un criterio predefinito o il criterio creato.

È inoltre possibile catalogare i backup del database Oracle utilizzando Oracle Recovery Manager (RMAN) se è stata attivata la catalogazione durante la creazione di una policy. La catalogazione (RMAN) è supportata solo per i database su Azure NetApp Files. I backup catalogati possono essere utilizzati in seguito per operazioni di ripristino a livello di blocco o tablespace point-in-time. Il database deve essere in stato montato o superiore per la catalogazione.

Creare policy per proteggere il database Oracle

È possibile creare policy se non si desidera modificare le policy predefinite.

Fasi

1. Nella pagina applicazioni, dall'elenco a discesa Impostazioni, selezionare **Criteri**.
2. Fare clic su **Crea policy**.
3. Specificare un nome di policy.

4. (Facoltativo) modificare il formato del nome del backup.
5. Specificare la pianificazione e i dettagli di conservazione.
6. Se hai selezionato *daily* e *settimanalmente* come programma e desideri attivare la catalogazione RMAN, seleziona **Catalog backup with Oracle Recovery Manager (RMAN)**.
7. (Facoltativo) inserire il percorso post-script e il valore di timeout per il post-script che verrà eseguito dopo il backup corretto, ad esempio la copia dello snapshot nello storage secondario.

In alternativa, è possibile specificare anche gli argomenti.

I post-script devono essere contenuti nel percorso `/var/opt/snapcenter/spl/scripts`.

Lo script post supporta un set di variabili di ambiente.

Variabile ambientale	Descrizione
SC_ORACLE_SID	Specifica il SID del database Oracle.
HOST_SC	Specifica il nome host del database
NOME_BACKUP_SC	Specifica il nome del backup. Il nome del backup dei dati e il nome del backup del registro vengono concatenati mediante delimitatori.
NOME_POLICY_BACKUP_SC	Specifica il nome del criterio utilizzato per creare il backup.
PERCORSO_COMPLETO_VOLUME_DATI_PRIMARI_SC	<p>Specifica i percorsi dei volumi di dati concatenati utilizzando "," come delimitatore. Per i volumi Azure NetApp Files, le informazioni vengono concatenate utilizzando "/"</p> <p>— /Subscriptions/{subscription_id}/resourceGroups/{resource_group}/provider/{provider}/netAppAccounts/{anfaccount}/capacityPools/{Capacity_pool}/volumename{}</p>
SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH	<p>Specifica i percorsi dei volumi del log di archiviazione concatenati utilizzando "," come delimitatore. Per i volumi Azure NetApp Files, le informazioni vengono concatenate utilizzando "/"</p> <p>— /Subscriptions/{subscription_id}/resourceGroups/{resource_group}/provider/{provider}/netAppAccounts/{anfaccount}/capacityPools/{Capacity_pool}/volumename{}</p>

8. Fare clic su **Create** (Crea).


Configurare il repository del catalogo RMAN

È possibile configurare il database del catalogo di ripristino come repository del catalogo RMAN. Se non si configura il repository, per impostazione predefinita, il file di controllo del database di destinazione diventa il repository del catalogo RMAN.

Prima di iniziare

Registrare manualmente il database di destinazione con il database del catalogo RMAN.

Fasi

1. Nella pagina applicazioni, fare clic su **...** > **Visualizza dettagli**.
2. Nella sezione Database details (Dettagli database), fare clic su  Per configurare il repository del catalogo RMAN.
3. Specificare le credenziali per catalogare i backup con RMAN e il nome TNS (transparent Network substrate) del database di ripristino del catalogo.
4. Fare clic su **Configura**.

Creare un backup del database Oracle

È possibile assegnare un criterio predefinito o creare un criterio e assegnarlo al database. Una volta assegnato il criterio, i backup vengono creati in base alla pianificazione definita nel criterio.



Quando si creano diskgroup ASM su Amazon FSX per NetApp ONTAP o Cloud Volumes ONTAP, assicurarsi che non vi siano volumi comuni tra i diskgroup. Ogni gruppo di dischi deve disporre di volumi dedicati.

Fasi

1. Nella pagina applicazioni, se il database non è protetto mediante criteri, fare clic su **Assegna policy**.

Se il database è protetto mediante uno o più criteri, è possibile assegnare ulteriori criteri facendo clic su **...** > **Assegna policy**.
2. Selezionare il criterio e fare clic su **Assegna**.

I backup verranno creati in base alla pianificazione definita nella policy. Se è stato abilitato il catalogo RMAN nella policy, il backup alla fine del workflow avvierà l'operazione di catalogazione come un lavoro separato. L'avanzamento della catalogazione è visibile da Job Monitor. Una volta completata la catalogazione, **Backup Details** mostrerà lo stato del catalogo per ciascun backup.



L'account del servizio (*SnapCenter-account-`<account_id>`*) viene utilizzato per eseguire le operazioni di backup pianificate.

Creazione di backup on-demand del database Oracle

Dopo aver assegnato il criterio, è possibile creare un backup on-demand dell'applicazione.

Fasi

1. Nella pagina applicazioni, fare clic su **...** Corrispondente all'applicazione e fare clic su **Backup on-**

Demand.

2. Se all'applicazione sono assegnati più criteri, selezionare il criterio, il livello di conservazione e fare clic su **Create Backup** (Crea backup).

Se è stato abilitato il catalogo RMAN nella policy, il backup alla fine del workflow avvierà l'operazione di catalogazione come un lavoro separato. L'avanzamento della catalogazione è visibile da Job Monitor. Una volta completata la catalogazione, **Backup Details** mostrerà lo stato del catalogo per ciascun backup.

Limitazioni

- Non supporta snapshot di gruppi di coerenza per database Oracle che risiedono su più gruppi di dischi ASM con sovrapposizione di volumi FSX
- Se i database Oracle si trovano su Amazon FSX per NetApp ONTAP o Cloud Volumes ONTAP e sono configurati su ASM, assicurarsi che i nomi SVM siano univoci nei sistemi FSX. Se si dispone dello stesso nome SVM nei sistemi FSX, il backup dei database Oracle che risiedono su tali SVM non è supportato.
- Dopo il ripristino di un database di grandi dimensioni (250 GB o superiore), se si esegue un backup online completo sullo stesso database, l'operazione potrebbe non riuscire e causare il seguente errore:
failed with status code 500, error
{\"error\":{\"code\":\"app_internal_error\",\"message\":\"Failed to create snapshot. Reason: Snapshot operation not allowed due to clones backed by snapshots. Try again after sometime.\"}}

Per informazioni su come risolvere questo problema, fare riferimento a: ["Operazione Snapshot non consentita a causa di cloni supportati da snapshot"](#).

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.